CLAIMS

What is Claimed is:

1. A method for remote incremental program verification, said method comprising:

receiving content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer, a device issuer and a trusted post-issuance installer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data, said verification including determining binary compatibility of earlier program unit implementations with later program unit implementations;

installing said content on a resource-constrained device;

issuing said resource-constrained device to an end user; and

allowing post-issuance installation of verified content on said resource-constrained device by said trusted post-issuance installer, said post-installation occurring after said issuance.

2. The method of claim 1 wherein said verification further comprises:

receiving a second version of said first program unit implementation and a second version of said first program unit API definition file, said second version being a revised version of said first version;

verifying said second version of said first program unit implementation, including

indicating a verification error when said second version of said first program unit implementation is not internally consistent; and

indicating a verification error when said second version of said first program unit implementation is inconsistent with said second version of said first program unit API definition file; and

verifying said second version of said first program unit implementation is binary compatible with said first version of said first program unit implementation, including indicating a verification error when said first version of said first program unit API definition file is incompatible with said second version of said first program unit API definition file.

3. The method of claim 2, further comprising:

indicating a verification error when a second program unit implementation that references said first program unit is inconsistent with said first version of said first program unit API definition file; and

indicating said second program unit implementation is verified with said second version of said first program unit API definition file when said second version of

said first program unit implementation is compatible with said first version of said first program unit implementation.

4. The method of claim 3, further comprising:

indicating said second program unit implementation is verified with said second version of said first program unit implementation when said second program unit implementation is verified with said second version of said first program unit API definition file.

5. The method of claim 2 wherein said first version of said first program unit API definition file is binary compatible with said second version of said first program unit API definition file when said second version of said first program unit API definition file includes a superset of each element in said first version of said first program unit API definition file.

6. The method of claim 2 wherein

said trusted post-issuance installer verifies a new program unit, and

said trusted post-issuance installer installs said verified new program unit on said resource-constrained device.

7. The method of claim 6 wherein post-issuance verification is performed on a resource-rich device.

8. The method of claim 6 wherein post-issuance verification is performed on a terminal device.

9. The method of claim 6 wherein said verification is performed by the provider of said new program unit.

10. The method of claim 6 wherein said verification is performed by said applet provider.

11. The method of claim 6 wherein said verification is performed by said device manufacturer.

12. The method of claim 6 wherein said verification is performed by said device issuer.

13. The method of claim 6 wherein said verification is performed by said applet provider and said device manufacturer.

14. The method of claim 6 wherein said verification is performed by said applet provider and said device issuer.

15. The method of claim 6 wherein said verification is performed by said device manufacturer and said device issuer.

16. The method of claim 6 wherein said verification is performed by said applet provider, said device manufacturer and said device issuer.

17. The method of claim 6 wherein said verification is performed by said applet provider, said device manufacturer, said device issuer and said trusted post-issuance installer.

18. The method of claim 6 wherein said verification is performed by said device manufacturer, said device issuer and said trusted post-issuance installer.

19. The method of claim 6 wherein said verification is performed by said device manufacturer and said trusted post-issuance installer.

20. The method of claim 6 wherein said verification is performed by said device issuer and said trusted post-issuance installer.

21. The method of claim 6 wherein post-issuance verification is performed on a resource-rich device.

22. The method of claim 6 wherein post-issuance verification is performed on a terminal device.

23. A method for remote incremental program verification, said method comprising:

receiving content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer, a device issuer and an untrusted post-issuance installer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data, said verification including determining binary compatibility of earlier program unit implementations with later program unit implementations;

installing said content on a resource-constrained device;

issuing said resource-constrained device to an end user; and

allowing post-issuance installation of verified content on said resource-constrained device by said untrusted post-issuance installer, said post-installation occurring after said issuance.

24. The method of claim 23 wherein said verification further comprises:

receiving a second version of said first program unit implementation and a second version of said first program unit API definition file, said second version being a revised version of said first version; and

verifying said second version of said first program unit implementation, including

determining whether said second version of said first program unit implementation is internally consistent; and

determining whether said second version of said first program unit implementation is consistent with said second version of said first program unit API definition file; and

verifying said second version of said first program unit implementation is binary compatible with said first version of said first program unit implementation by comparing said first version of said first program unit API definition file and said second version of said first program unit API definition file.

25. The method of claim 24, further comprising:

determining whether a second program unit implementation that references said first program unit is consistent with said first version of said first program unit API definition file; and

indicating said second program unit implementation is verified with said second version of said first program unit API definition file when said second version of

said first program unit implementation is compatible with said first version of said first program unit implementation.

26. The method of claim 25, further comprising:

indicating said second program unit implementation is verified with said second version of said first program unit implementation when said second program unit implementation is verified with said second version of said first program unit API definition file.

27. The method of claim 24 wherein said first version of said first program unit API definition file is binary compatible with said second version of said first program unit API definition file when said second version of said first program unit API definition file includes a superset of each element in said first version of said first program unit API definition file.

28. The method of claim 24 wherein

said untrusted post-issuance installer verifies a new program unit; and

said untrusted post-issuance installer installs said verified new program unit on said resource-constrained device.

29. The method of claim 24 wherein post-issuance verification is performed on a resource-rich device.

30. The method of claim 24 wherein post-issuance verification is performed on a terminal device.

31. The method of claim 24 wherein said verification is performed by the provider of said new program unit.

32. The method of claim 24 wherein said verification is performed by said applet provider.

33. The method of claim 24 wherein said verification is performed by said device manufacturer.

34. The method of claim 24 wherein said verification is performed by said device issuer.

35. The method of claim 24 wherein said verification is performed by said applet provider and said device manufacturer.

36. The method of claim 24 wherein said verification is performed by said applet provider and said device issuer.

37. The method of claim 24 wherein said verification is performed by said device manufacturer and said device issuer.

38. The method of claim 24 wherein said verification is performed by said applet provider, said device manufacturer and said device issuer.

39. The method of claim 24 wherein said verification is performed by said applet provider, said device manufacturer, said device issuer and said untrusted post-issuance installer.

40. The method of claim 24 wherein said verification is performed by said device manufacturer, said device issuer and said untrusted post-issuance installer.

41. The method of claim 24 wherein said verification is performed by said device manufacturer and said untrusted post-issuance installer.

42. The method of claim 24 wherein said verification is performed by said device issuer and said untrusted post-issuance installer.

43. The method of claim 24 wherein post-issuance verification is performed on a resource-rich device.

44. The method of claim 24 wherein post-issuance verification is performed on a terminal device.

45. A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform program verification, comprising:

receiving content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer, a device issuer and a trusted post-issuance installer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data, said verification including determining binary compatibility of earlier program unit implementations with later program unit implementations;

installing said content on a resource-constrained device;

issuing said resource-constrained device to an end user; and

allowing post-issuance installation of verified content on said resource-constrained device by said trusted post-issuance installer, said post-installation occurring after said issuance.

46. The program storage device of claim 45 wherein said verification further comprises:

receiving a second version of said first program unit implementation and a second version of said first program unit API definition file, said second version being a revised version of said first version;

verifying said second version of said first program unit implementation, including

indicating a verification error when said second version of said first program unit implementation is not internally consistent; and

indicating a verification error when said second version of said first program unit implementation is inconsistent with said second version of said first program unit API definition file; and

verifying said second version of said first program unit implementation is binary compatible with said first version of said first program unit implementation including indicating a verification error when said first version of said first program unit API definition file is incompatible with said second version of said first program unit API definition file.

47. The program storage device of claim 46, further comprising:

indicating a verification error when a second program unit implementation that references said first program unit is inconsistent with said first version of said first program unit API definition file; and

indicating said second program unit implementation is verified with said second version of said first program unit API definition file when said second version of said first program unit implementation is compatible with said first version of said first program unit implementation.

48. The program storage device of claim 47, further comprising:

indicating said second program unit implementation is verified with said second version of said first program unit implementation when said second program unit implementation is verified with said second version of said first program unit API definition file.

49. The program storage device of claim 46 wherein said first version of said first program unit API definition file is binary compatible with said second version of said first program unit API definition file when said second version of said first program unit API definition file includes a superset of each element in said first version of said first program unit API definition file.

50. The program storage device of claim 46 wherein

said trusted post-issuance installer verifies a new program unit; and

said trusted post-issuance installer installs said verified new program unit on said resource-constrained device.

51. The program storage device of claim 50 wherein post-issuance verification is performed on a resource-rich device.

52. The program storage device of claim 50 wherein post-issuance verification is performed on a terminal device.

53. The program storage device of claim 50 wherein said verification is performed by the provider of said new program unit.

54. A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform program verification, comprising:

receiving content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer, a device issuer and an untrusted post-issuance installer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program

units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data, said verification including determining binary compatibility of earlier program unit implementations with later program unit implementations;

installing said content on a resource-constrained device;

issuing said resource-constrained device to an end user; and

allowing post-issuance installation of verified content on said resource-constrained device by said untrusted post-issuance installer, said post-installation occurring after said issuance.

55. The program storage device of claim 54 wherein said verification further comprises:

receiving a second version of said first program unit implementation and a second version of said first program unit API definition file, said second version being a revised version of said first version; and

verifying said second version of said first program unit implementation, including

indicating a verification error when said second version of said first program unit implementation is not internally consistent; and

indicating a verification error when said second version of said first program unit implementation is inconsistent with said second version of said first program unit API definition file; and

verifying said second version of said first program unit implementation is binary compatible with said first version of said first program unit

implementation including indicating a verification error when said first version of said first program unit API definition file is incompatible when said second version of said first program unit API definition file.

56. The program storage device of claim 55, further comprising:

indicating a verification error when a second program unit implementation that references said first program unit is inconsistent with said first version of said first program unit API definition file; and

indicating said second program unit implementation is verified with said second version of said first program unit API definition file when said second version of said first program unit implementation is compatible with said first version of said first program unit implementation.

57. The program storage device of claim 56, further comprising:

indicating said second program unit implementation is verified with said second version of said first program unit implementation when said second program unit implementation is verified with said second version of said first program unit API definition file.

58. The program storage device of claim 55 wherein said first version of said first program unit API definition file is binary compatible with said second version of said first program unit API definition file when said second version of said first program

unit API definition file includes a superset of each element in said first version of said first program unit API definition file.

59. The program storage device of claim 55 wherein

said untrusted post-issuance installer verifies a new program unit; and

said untrusted post-issuance installer installs said verified new program unit on said resource-constrained device.

60. The program storage device of claim 55 wherein post-issuance verification is performed on a resource-rich device.

61. The program storage device of claim 55 wherein post-issuance verification is performed on a terminal device.

62. The program storage device of claim 55 wherein said verification is performed by the provider of said new program unit.

63. A system for executing a software application, the system comprising:

a computing system that generates executable code, comprising means for

receiving content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer, a device issuer and a trusted post-issuance installer, said content including at least one

program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data, said verification including determining binary compatibility of earlier program unit implementations with later program unit implementations;

means for installing said content on a resource-constrained device;

means for issuing said resource-constrained device to an end user; and

means for allowing post-issuance installation of verified content on said resource-constrained device by said trusted post-issuance installer, said post-installation occurring after said issuance.

64. The system of claim 63 wherein said verification further comprises:

means for receiving a second version of said first program unit implementation and a second version of said first program unit API definition file, said second version being a revised version of said first version;

means for verifying said second version of said first program unit implementation, including

means for indicating a verification error when said second version of said first program unit implementation is not internally consistent; and

means for indicating a verification error when said second version of said first program unit implementation is inconsistent with said second version of said first program unit API definition file; and

means for verifying said second version of said first program unit implementation is binary compatible with said first version of said first program unit implementation including indicating a verification error when said first version of said first program unit API definition file is incompatible with said second version of said first program unit API definition file.

65. The system of claim 64, further comprising:

means for indicating a verification error when a second program unit implementation that references said first program unit is inconsistent with said first version of said first program unit API definition file; and

means for indicating said second program unit implementation is verified with said second version of said first program unit API definition file when said second version of said first program unit implementation is compatible with said first version of said first program unit implementation.

66. The system of claim 65, further comprising:

means for indicating said second program unit implementation is verified with said second version of said first program unit implementation when said second

program unit implementation is verified with said second version of said first program unit API definition file.

67. The system of claim 64 wherein said first version of said first program unit API definition file is binary compatible with said second version of said first program unit API definition file when said second version of said first program unit API definition file includes a superset of each element in said first version of said first program unit API definition file.

68. The system of claim 64 wherein

said trusted post-issuance installer verifies a new program unit; and

said trusted post-issuance installer installs said verified new program unit on said resource-constrained device.

69. The system of claim 68 wherein post-issuance verification is performed on a resource-rich device.

70. The system of claim 68 wherein post-issuance verification is performed on a terminal device.

71. The system of claim 68 wherein said verification is performed by the provider of said new program unit.

72. The system of claim 68 wherein said verification is performed by said applet provider.

73. A system for executing a software application, the system comprising:

a computing system that generates executable code, comprising means for receiving content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer, a device issuer and an untrusted post-issuance installer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data, said verification including determining binary compatibility of earlier program unit implementations with later program unit implementations;

means for installing said content on a resource-constrained device;

means for issuing said resource-constrained device to an end user; and

means for allowing post-issuance installation of verified content on said resource-constrained device by said untrusted post-issuance installer, said post-installation occurring after said issuance.

74. The system of claim 73 wherein said verification further comprises:

means for receiving a second version of said first program unit implementation and a second version of said first program unit API definition file, said second version being a revised version of said first version;

means for verifying said second version of said first program unit implementation, including

means for indicating a verification error when said second version of said first program unit implementation is not internally consistent; and

means for indicating a verification error when said second version of said first program unit implementation is inconsistent with said second version of said first program unit API definition file; and

means for verifying said second version of said first program unit implementation is binary compatible with said first version of said first program unit implementation including indicating a verification error when said first version of said first program unit API definition file is incompatible with said second version of said first program unit API definition file.

75. The system of claim 74, further comprising:

means for indicating a verification error when a second program unit implementation that references said first program unit is inconsistent with said first version of said first program unit API definition file; and

means for indicating said second program unit implementation is verified with said second version of said first program unit API definition file when said second version of said first program unit implementation is compatible with said first version of said first program unit implementation.

76. The system of claim 75, further comprising:

means for indicating said second program unit implementation is verified with said second version of said first program unit implementation when said second program unit implementation is verified with said second version of said first program unit API definition file.

77. The system of claim 74 wherein said first version of said first program unit API definition file is binary compatible with said second version of said first program unit API definition file when said second version of said first program unit API definition file includes a superset of each element in said first version of said first program unit API definition file.

78. The system of claim 74 wherein

said untrusted post-issuance installer verifies a new program unit; and

said untrusted post-issuance installer installs said verified new program unit on said resource-constrained device.

79. The system of claim 74 wherein post-issuance verification is performed on a resource-rich device.

80. The system of claim 74 wherein post-issuance verification is performed on a terminal device.

81. The system of claim 78 wherein said verification is performed by the provider of said new program unit.

82. A resource-constrained device, comprising:

memory for providing content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer, a device issuer and a trusted post-issuance installer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code

corresponding to said API definition file, said executable code including type specific instructions and data, said verification including determining binary compatibility of earlier program unit implementations;

an installer device for installation of said content on said resource-constrained device, said installation including installation of initial content and installation of additional content by said trusted post-issuance installer after said resource-constrained device is issued to an end user; and

a virtual machine that is capable of executing instructions included within said content.

83. The resource-constrained device of claim 82 wherein said resource-constrained device comprises a smart card.

84. The resource-constrained device of claim 83 wherein said virtual machine is Java Card™-compliant.

85. A resource-constrained device, comprising:

memory for providing content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer, a device issuer and an untrusted post-issuance installer, said content including at

least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data, said verification including determining binary compatibility of earlier program unit implementations with later program unit implementations;

an installer device for installation of said content on said resource-constrained device, said installation including installation of initial content and installation of additional content by said untrusted post-issuance installer after said resource-constrained device is issued to an end user; and

a virtual machine that is capable of executing instructions included within said content.

86. The resource-constrained device of claim 85 wherein said resource-constrained device comprises a smart card.

87. The resource-constrained device of claim 85 wherein said virtual machine is Java Card™-compliant.